

Comparing Kalman Filters and Observers for Dynamic State Estimation with Model Uncertainty and Malicious Cyber Attacks

Junjian Qi, *Member, IEEE*, Ahmad F. Taha, *Member, IEEE*, and Jianhui Wang, *Senior Member, IEEE*

Abstract—Kalman filters and observers are two main classes of dynamic state estimation (DSE) routines. Power system DSE has been implemented by various Kalman filters, such as the extended Kalman filter (EKF) and the unscented Kalman filter (UKF). In this paper, we discuss two challenges for an effective power system DSE: (a) model uncertainty and (b) potential cyber attacks. To address this, the cubature Kalman filter (CKF) and a nonlinear observer are introduced and implemented. Various Kalman filters and the observer are then tested on the 16-machine, 68-bus system given realistic scenarios under model uncertainty and different types of cyber attacks against synchrophasor measurements. It is shown that CKF and the observer are more robust to model uncertainty and cyber attacks than their counterparts. Based on the tests, a thorough qualitative comparison is also performed for Kalman filter routines and observers.

Index Terms—Cubature Kalman filter, cyber attack, dynamic state estimation, extended Kalman filter, model uncertainty, observer, phasor measurement unit (PMU), unscented Kalman filter.

I. INTRODUCTION

STATE estimation is a crucial application in the energy management system (EMS). The well-known static state estimation (SSE) methods [1]–[5] assume that the power system is operating in quasi-steady state, based on which the static states—the voltage magnitude and phase angles of the buses—are estimated by using SCADA and/or synchrophasor measurements. SSE is critical for power system monitoring as it provides inputs for other EMS applications such as automatic generation control and optimal power flow.

However, SSE may not be sufficient for desirable situational awareness as the system states evolve more rapidly due to an increasing penetration of renewable generation and distributed energy resources. Therefore, dynamic state estimation (DSE) processes estimating the dynamic states (i.e., the internal states of generators) by using highly synchronized PMU measurements with high sampling rates will be critical for the wide-area monitoring, protection, and control of power systems.

For both SSE and DSE, two significant challenges make their practical application significantly difficult. First, the

system model and parameters used for estimation can be inaccurate, which is often called *model uncertainty* [6], consequently deteriorating estimation in some scenarios. Second, the measurements used for estimation are vulnerable to cyber attacks, which in turn leads to compromised measurements that can greatly mislead the estimation.

For the first challenge, there are recent efforts on validating the dynamic model of the generator and calibrating its parameters [7]–[9], which DSE can be based on. However, model validation itself can be very challenging. Hence, it is a more viable solution to improve the estimators by making them more robust to the model uncertainty.

For the second challenge, false data injection attacks targeted against SSE are proposed in [10]. In [11], a probabilistic risk mitigation model is presented for cyber attacks against PMU networks, focusing on topological observability of SSE. However, in this paper we discuss cyber attacks against DSE and estimators that are robust to cyber attacks.

As for the approaches for performing DSE, there are mainly two classes of methods that have been proposed:

- 1) *Stochastic Estimators*: given a discrete-time representation of a dynamical system, the observed measurements, and the statistical information on process noise and measurement noise, Kalman filter and its many derivatives have been proposed that calculate the Kalman gain as a function of the relative certainty of the current state estimate and the measurements [12]–[16].
- 2) *Deterministic Observers*: given a continuous- or discrete-time dynamical system depicted by state-space matrices, a combination of matrix equalities and inequalities are solved, while guaranteeing asymptotic (or bounded) estimation error. The solution to these equations is often matrices that are used in an observer to estimate states and other dynamic quantities [17]–[19].

For power systems, DSE has been implemented by several stochastic estimators, such as extended Kalman filter (EKF) [20], [21], unscented Kalman filter (UKF) [22]–[25], square-root unscented Kalman filter (SR-UKF) [26]–[28], extended particle filter [29], [30], and ensemble Kalman filter [31]. While these techniques produce good estimation under nominal conditions, most of them lack the ability to deal with significant model uncertainty and malicious cyber attacks.

The goal of this paper is to present alternatives that address these major limitations. To achieve this, we study DSE by utilizing recently developed Kalman filters and nonlinear observers. The contributions of this paper include:

This work is supported in part by U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability.

J. Qi and J. Wang are with the Energy Systems Division, Argonne National Laboratory, Argonne, IL 60439 USA (e-mails: jqj@anl.gov; jianhui.wang@anl.gov).

A. F. Taha is with the Department of Electrical and Computer Engineering, the University of Texas at San Antonio, San Antonio, TX 78249 and was a research intern with the Energy Systems Division, Argonne National Laboratory, Argonne, IL 60439 USA in 2015 (e-mail: ahmad.taha@utsa.edu).

- 1) Introducing cubature Kalman filter (CKF) [16] that possesses an important virtue of mathematical rigor rooted in the third-degree spherical-radial cubature rule for numerically computing Gaussian-weighted integrals;
- 2) Presenting observers for DSE of nonlinear power systems with model uncertainties and cyber attacks;
- 3) Comparing the strengths and limitations of different estimation methods for DSE with significant model uncertainty and cyber attacks.

The remainder of this paper is organized as follows. In Section II, we discuss the nonlinear dynamics of the multi-machine power system. The physical and technical depictions of the model uncertainty and attack-threat model are introduced in Section III. The CKF and one dynamic observer are introduced in Sections IV and V. Then, numerical results are given in Section VI. Finally, insightful remarks and conclusions are presented in Sections VII and VIII.

II. NONLINEAR MULTI-MACHINE POWER SYSTEM MODEL

Here we briefly discuss the power system model used for DSE. Each of the G generators is described by the fourth-order transient model in local d - q reference frame:

$$\begin{cases} \dot{\delta}_i = \omega_i - \omega_0 \\ \dot{\omega}_i = \frac{\omega_0}{2H_i}(T_{mi} - T_{ei} - \frac{K_{Di}}{\omega_0}(\omega_i - \omega_0)) \\ \dot{e}'_{qi} = \frac{1}{T'_{d0i}}(E_{fdi} - e'_{qi} - (x_{di} - x'_{di})i_{di}) \\ \dot{e}'_{di} = \frac{1}{T'_{q0i}}(-e'_{di} + (x_{qi} - x'_{qi})i_{qi}) \end{cases} \quad (1)$$

where i is the generator serial number, δ_i is the rotor angle, ω_i is the rotor speed in rad/s, and e'_{qi} and e'_{di} are the transient voltage along q and d axes; i_{qi} and i_{di} are stator currents at q and d axes; T_{mi} is the mechanical torque, T_{ei} is the electric air-gap torque, and E_{fdi} is the internal field voltage; ω_0 is the rated value of angular frequency, H_i is the inertia constant, and K_{Di} is the damping factor; T'_{q0i} and T'_{d0i} are the open-circuit time constants for q and d axes; x_{qi} and x_{di} are the synchronous reactance and x'_{qi} and x'_{di} are the transient reactance respectively at the q and d axes.

The T_{mi} and E_{fdi} in (1) are considered as inputs. The set of generators where PMUs are installed is denoted by \mathcal{G}_P . For generator $i \in \mathcal{G}_P$, the terminal voltage phasor $E_{ti} = e_{Ri} + j e_{Ii}$ and current phasor $I_{ti} = i_{Ri} + j i_{Ii}$ can be measured and are used as the outputs. Correspondingly, the state vector $\mathbf{x} \in \mathbb{R}^n$, input vector $\mathbf{u} \in \mathbb{R}^v$, and output vector $\mathbf{y} \in \mathbb{R}^p$ are

$$\mathbf{x} = [\delta^\top \quad \omega^\top \quad e_q'^\top \quad e_d'^\top]^\top \quad (2a)$$

$$\mathbf{u} = [T_m^\top \quad E_{fd}^\top]^\top \quad (2b)$$

$$\mathbf{y} = [e_R^\top \quad e_I^\top \quad i_R^\top \quad i_I^\top]^\top. \quad (2c)$$

The T_{ei} , i_{di} , and i_{qi} can be written as functions of \mathbf{x} :

$$\Psi_{Ri} = e'_{di} \sin \delta_i + e'_{qi} \cos \delta_i \quad (3a)$$

$$\Psi_{Ii} = e'_{qi} \sin \delta_i - e'_{di} \cos \delta_i \quad (3b)$$

$$I_{ti} = \bar{\mathbf{Y}}_i(\Psi_R + j\Psi_I) \quad (3c)$$

$$i_{Ri} = \text{Re}(I_{ti}) \quad (3d)$$

$$i_{Ii} = \text{Im}(I_{ti}) \quad (3e)$$

$$i_{qi} = \frac{S_B}{S_{Ni}}(i_{Ii} \sin \delta_i + i_{Ri} \cos \delta_i) \quad (3f)$$

$$i_{di} = \frac{S_B}{S_{Ni}}(i_{Ri} \sin \delta_i - i_{Ii} \cos \delta_i) \quad (3g)$$

$$e_{qi} = e'_{qi} - x'_{di} i_{di} \quad (3h)$$

$$e_{di} = e'_{di} + x'_{qi} i_{qi} \quad (3i)$$

$$T_{ei} = \frac{S_B}{S_{Ni}}(e_{qi} i_{qi} + e_{di} i_{di}). \quad (3j)$$

where $\Psi_i = \Psi_{Ri} + j\Psi_{Ii}$ is the voltage source, Ψ_R and Ψ_I are column vectors of all generators' Ψ_{Ri} and Ψ_{Ii} , e_{qi} and e_{di} are the terminal voltage at q and d axes, $\bar{\mathbf{Y}}_i$ is the i th row of the admittance matrix of the reduced network $\bar{\mathbf{Y}}$, and S_B and S_{Ni} are the system base MVA and the base MVA for generator i , respectively.

In (3), the outputs i_{Ri} and i_{Ii} are written as functions of \mathbf{x} . Similarly, the outputs e_{Ri} and e_{Ii} can also be written as function of \mathbf{x} :

$$e_{Ri} = e_{di} \sin \delta_i + e_{qi} \cos \delta_i \quad (4a)$$

$$e_{Ii} = e_{qi} \sin \delta_i - e_{di} \cos \delta_i. \quad (4b)$$

The dynamic model (1) can then be rewritten in a general state space form as

$$\begin{cases} \dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{u} + \phi(\mathbf{x}) \\ \mathbf{y} = \mathbf{h}(\mathbf{x}) \end{cases} \quad (5)$$

where

$$\mathbf{A} = \begin{bmatrix} \mathbf{I}_G & & & \\ & \text{diag}(-\frac{\mathbf{K}_D}{2H}) & & \\ & & \text{diag}(-\frac{1}{T'_{d0}}) & \\ & & & \text{diag}(-\frac{1}{T'_{q0}}) \end{bmatrix},$$

$$\mathbf{B} = \begin{bmatrix} & & & \\ & \text{diag}(\frac{\omega_0}{2H}) & & \\ & & \text{diag}(\frac{1}{T'_{d0}}) & \\ & & & \text{diag}(\frac{1}{T'_{q0}}) \end{bmatrix}, \quad \phi = \begin{bmatrix} -\omega_0 \mathbf{1}_G \\ \frac{\omega_0}{2H}(-\mathbf{T}_e + \mathbf{K}_D \mathbf{1}_n) \\ \frac{1}{T'_{d0}}(-(x_d - x'_d)i_d) \\ \frac{1}{T'_{q0}}((x_q - x'_q)i_q) \end{bmatrix},$$

and \mathbf{h} include functions (3d)–(3e) and (4) for all generators.

Note that the model presented here is used for DSE for which the real-time inputs are assumed to be unavailable and T_{mi} and E_{fdi} only take steady-state values, mainly because these inputs are difficult to measure [21], [24]. However, when we simulate the power system to mimic the real system dynamics, we model an IEEE Type DC1 excitation system and a simplified turbine-governor system for each generator and thus T_{mi} and E_{fdi} change with time due to the governor and the excitation control.

We do not directly use a detailed model including the exciter and governor as in [30] for the DSE mainly because 1) A good model should be simple enough to facilitate design [6], 2) it is harder to validate a more detailed model and there are also more parameters that need to be calibrated [7]–[9], and 3) the computational burden can be higher for a more detailed model, which may not satisfy the requirement of real-time estimation.

III. MODEL UNCERTAINTY AND CYBER ATTACKS

Here we discuss two great challenges for an effective DSE, which are the model uncertainty and potential cyber attacks.

A. Model Uncertainty

The term *model uncertainty* refers to the differences or errors between models and reality. Assuming that the dynamical models are perfectly accurate can generate sub-optimal control or estimation laws. Various control and estimation theory studies investigated methods that addresses the discrepancy between the actual physics and models. The model uncertainty can be caused by the following reasons.

- 1) **Unknown inputs:** The unknown inputs against the system dynamics include \mathbf{u}_d (representing the unknown plant disturbances), \mathbf{u}_u (denoting the unknown control inputs), and \mathbf{f}_a (depicting potential actuator faults). For simplicity, we can combine them into one unknown input quantity, \mathbf{w} , defined as $\mathbf{w} = [\mathbf{u}_d^\top \mathbf{u}_u^\top \mathbf{f}_a^\top]^\top \in \mathbb{R}^{m_2}$. Defining \mathbf{B}_w to be the known weight distribution matrix of the distribution of unknown inputs with respect to each state-equation. The term $\mathbf{B}_w \mathbf{w}$ models a general class of unknown inputs such as: nonlinearities, modeling uncertainties, noise, parameter variations, unmeasurable system inputs, model reduction errors, and actuator faults [32], [33]. For example, the equation $\dot{x}_1 = \delta_1 = \omega_1 - \omega_0$ most likely has no unknown inputs, as there is no modeling uncertainty related to that process. Hence, the first row of \mathbf{B}_w can be identically zero. The process dynamics under unknown inputs can be written as follows:

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{u} + \mathbf{B}_w \mathbf{w} + \phi(\mathbf{x}). \quad (6)$$

- 2) **Unavailable inputs:** As discussed in Section II, the real-time inputs \mathbf{u} in (1) can be unavailable, in which case the steady-states inputs \mathbf{u}_0 are used for estimation.
- 3) **Parameter inaccuracy:** The parameters in the system model can be inaccurate. For example, the reduced admittance matrix $\bar{\mathbf{Y}}$ can be inaccurate when a fault or the following topology change are not detected.

B. Cyber Attacks

The National Electric Sector Cybersecurity Organization Resource (NESCOR) developed cyber-security failure scenarios with corresponding impact analyses [34]. The WAMPAC failure scenarios motivate the research in this paper include: a) *Measurement Data (from PMUs) Compromised due to PDC Authentication Compromise* and b) *Communications Compromised between PMUs and Control Center* [34]. Specifically, we consider the following three types of attacks [34], [35].

- 1) **Data integrity attacks:** An adversary attempts to corrupt the content of either the measurement or the control signals. A specific example of data integrity attacks are Man-in-the-Middle attacks, where the adversary intercepts the measurement signals and modifies them in transit. For DSE the PMU measurements can be modified and corrupted.
- 2) **Denial of Service (DoS) attack:** An attacker attempts to introduce a denial in communication of measurement. The communication of a sensor could be jammed by flooding the network with spurious packets. For DSE the consequence can be that the updated measurements cannot be sent to the control center.

- 3) **Replay attacks:** A special case of data integrity attacks, where the attacker replays a previous snapshot of a valid communication packet sequence that contains measurements in order to deceive the system. For DSE the PMU measurements can be changed to be those in the past.

IV. KALMAN FILTERS FOR POWER SYSTEM DSE

Unlike many estimation methods that are either computationally unmanageable or require special assumptions about the form of the process and observation models, Kalman filter (KF) only utilizes the first two moments of the state (mean and covariance) in its update rule [12]. It consists of two steps: in prediction step, the filter propagates the estimate from last time step to current time step; in update step, the filter updates the estimate using collected measurements. KF was initially developed for linear systems while for power system DSE the system equations and outputs have strong nonlinearity. Thus variants of KF that can deal with nonlinear systems have been introduced, such as EKF and UKF. Here, we briefly introduce EKF and UKF, and give more details for cubature Kalman filter (CKF).

A. Extended Kalman Filter

Although EKF maintains the elegant and computationally efficient recursive update form of KF, it works well only in a ‘mild’ nonlinear environment, owing it to the first-order Taylor series approximation for nonlinear functions [16]. It is sub-optimal and can easily lead to divergence. Also, the linearization can be applied only if the Jacobian matrix exists and calculating Jacobian matrices can be difficult and error-prone. For DSE, EKF has been discussed in [20], [21].

B. Unscented Kalman Filter

The unscented transformation (UT) [36] is developed to address the deficiencies of linearization by providing a more direct and explicit mechanism for transforming mean and covariance information. Based on UT, Julier et al. [14], [15] propose the UKF as a derivative-free alternative to EKF. The Gaussian distribution is represented by a set of deterministically chosen sample points called sigma points. The UKF has been applied to power system DSE, for which no linearization or calculation of Jacobian matrices is needed [22]–[25].

However, for the sigma-points, the stem at the center (the mean) is highly significant as it carries more weight which is usually negative for high-dimensional systems. Therefore, the UKF is supposed to encounter numerical instability troubles when used in high-dimensional problems. Several techniques including the square-root unscented Kalman filter (SR-UKF) have been proposed to solve this problem [26]–[28].

C. Cubature Kalman Filter

EKF and UKF can suffer from the curse of dimensionality while becoming detrimental in high-dimensional state-space models of size twenty or more—especially when there are high

degree of nonlinearities in the equations that describe the state-space model [16], [37]. Making use of the spherical-radial cubature rule, Arasaratnam et al. [16] propose CKF, which possesses an important virtue of mathematical rigor rooted in the third-degree spherical-radial cubature rule for numerically computing Gaussian-weighted integrals.

A nonlinear system (without model uncertainty or attack vectors) can be written in discrete-time form as

$$\begin{aligned} \mathbf{x}_k &= \mathbf{f}(\mathbf{x}_{k-1}, \mathbf{u}_{k-1}) + \mathbf{q}_{k-1} \\ \mathbf{y}_k &= \mathbf{h}(\mathbf{x}_k, \mathbf{u}_k) + \mathbf{r}_k \end{aligned}$$

where $\mathbf{x}_k \in \mathbb{R}^n$, $\mathbf{u}_k \in \mathbb{R}^v$, and $\mathbf{y}_k \in \mathbb{R}^p$ are states, inputs, and observed measurements at time step k ; the estimated mean and estimated covariance of the estimation error are \mathbf{m} and \mathbf{P} ; \mathbf{f} and \mathbf{h} are vectors consisting of nonlinear state transition functions and measurement functions; $\mathbf{q}_{k-1} \sim N(0, \mathbf{Q}_{k-1})$ is the Gaussian process noise at time step $k-1$; $\mathbf{r}_k \sim N(0, \mathbf{R}_k)$ is the Gaussian measurement noise at time step k ; and \mathbf{Q}_{k-1} and \mathbf{R}_k are covariance matrices of \mathbf{q}_{k-1} and \mathbf{r}_k .

The procedure of CKF consists of a prediction step and an update step and is summarized in Algorithms 1 and 2. Similar to other Kalman filters, in prediction step CKF propagates the estimate from last time step to current time step and in update step it updates the estimate using collected measurements.

Similar to UKF, CKF also uses a weighted set of symmetric points to approximate the Gaussian distribution. But the cubature-point set obtained in Step 1 of Algorithm 1 does not have a stem at the center and thus does not have the numerical instability problem of UKF discussed in Section IV-B.

Algorithm 1 CKF Algorithm: Prediction Steps

draw cubature points from the intersections of the n dimensional unit sphere and the Cartesian axes.

$$\boldsymbol{\xi}_i = \begin{cases} \sqrt{n} \mathbf{e}_i, & i = 1, \dots, n \\ -\sqrt{n} \mathbf{e}_{i-n}, & i = n+1, \dots, 2n \end{cases}$$

where \mathbf{e}_i is a vector with dimension n , whose i th element is one and the other elements are zero.

propagate the cubature points. The matrix square root is the lower triangular cholesky factor

$$\mathbf{X}_{i,k-1|k-1} = \sqrt{\mathbf{P}_{k-1|k-1}} \boldsymbol{\xi}_i + \mathbf{m}_{k-1|k-1}.$$

evaluate the cubature points with dynamic model function

$$\mathbf{X}_{i,k|k-1}^* = \mathbf{f}(\mathbf{X}_{i,k-1|k-1}).$$

estimate the predicted state mean

$$\mathbf{m}_{k|k-1} = \frac{1}{2n} \sum_{i=1}^{2n} \mathbf{X}_{i,k|k-1}^*.$$

estimate the predicted error covariance

$$\mathbf{P}_{k|k-1} = \frac{1}{2n} \sum_{i=1}^{2n} \mathbf{X}_{i,k|k-1}^* \mathbf{X}_{i,k|k-1}^{*\top} - \mathbf{m}_{k|k-1} \mathbf{m}_{k|k-1}^\top + \mathbf{Q}_{k-1}.$$

V. NONLINEAR OBSERVERS FOR POWER SYSTEM DSE

Dynamic observers have been thoroughly investigated for different classes of systems. To mention a few, they have been developed for linear time-invariant (LTI) systems, nonlinear time-invariant (NLTI) systems, LTI and NLTI systems with unknown inputs, sensor and actuator faults, stochastic dynamical systems, and hybrid systems [17], [18].

Algorithm 2 CKF Algorithm: Update Steps

draw cubature points from the intersections of the n dimensional unit sphere and the Cartesian axes.

propagate the cubature points

$$\mathbf{X}_{i,k|k-1} = \sqrt{\mathbf{P}_{k|k-1}} \boldsymbol{\xi}_i + \mathbf{m}_{k|k-1}.$$

evaluate cubature points using measurement function

$$\mathbf{Y}_{i,k|k-1} = \mathbf{h}(\mathbf{X}_{i,k|k-1}).$$

estimate the predicted measurement

$$\hat{\mathbf{y}}_{k|k-1} = \frac{1}{2n} \sum_{i=1}^{2n} \mathbf{Y}_{i,k|k-1}.$$

estimate the innovation covariance matrix

$$\mathbf{S}_{k|k-1} = \frac{1}{2n} \sum_{i=1}^{2n} \mathbf{Y}_{i,k|k-1} \mathbf{Y}_{i,k|k-1}^\top - \hat{\mathbf{y}}_{k|k-1} \hat{\mathbf{y}}_{k|k-1}^\top + \mathbf{R}_k.$$

estimate the cross-covariance matrix

$$\mathbf{P}_{xy,k|k-1} = \frac{1}{2n} \sum_{i=1}^{2n} \mathbf{X}_{i,k-1|k-1} \mathbf{Y}_{i,k|k-1}^\top - \mathbf{m}_{k|k-1} \hat{\mathbf{y}}_{k|k-1}^\top.$$

calculate the Kalman gain

$$\mathbf{K}_k = \mathbf{P}_{xy,k|k-1} \mathbf{S}_{k|k-1}^{-1}.$$

estimate the updated state

$$\mathbf{m}_{k|k} = \mathbf{m}_{k|k-1} + \mathbf{K}_k (\mathbf{y}_k - \hat{\mathbf{y}}_k).$$

estimate the updated error covariance

$$\mathbf{P}_{k|k} = \mathbf{P}_{k|k-1} - \mathbf{K}_k \mathbf{P}_{yy,k|k-1} \mathbf{K}_k^\top.$$

Most observers utilize the plant's outputs and inputs to generate real-time estimates of the plant states, unknown inputs, and sensor faults. The cornerstone is the innovation function—sometimes a simple gain matrix designed to nullify the effect of unknown inputs and faults. Linear and nonlinear functional observers, sliding-mode observers, unknown input observers, and observers for fault detection and isolation are all examples on developed observers for different classes of systems, under different assumptions [19].

In comparison with KF techniques, observers have not been utilized for power system DSE. However, they inherently possess the theoretical, technical, and computational capabilities to perform good estimation of the power system's dynamic states. As for implementation, observers are simpler than KFs. For observers, matrix gains are computed offline to guarantee the asymptotic stability of the estimation error.

Here, we present a recently developed observer in [38] that can be applied for DSE in power systems. This observer assumes that the nonlinear function $\phi(\mathbf{x})$ in (5) satisfies the one-sided Lipschitz condition. Specifically, there exists $\rho \in \mathbb{R}$ such that $\forall \mathbf{x}_1, \mathbf{x}_2$ in a region D including the origin with respect to the state \mathbf{x} , there is

$$\langle \phi(\mathbf{x}_1) - \phi(\mathbf{x}_2), \mathbf{x}_1 - \mathbf{x}_2 \rangle \leq \rho \|\mathbf{x}_1 - \mathbf{x}_2\|^2$$

where $\langle \cdot, \cdot \rangle$ is the inner product. Besides, the nonlinear function is also assumed to be quadratically inner-bounded as

$$\begin{aligned} (\phi(\mathbf{x}_1) - \phi(\mathbf{x}_2))^\top (\phi(\mathbf{x}_1) - \phi(\mathbf{x}_2)) &\leq \mu \|\mathbf{x}_1 - \mathbf{x}_2\|^2 \\ &+ \varphi \langle \phi(\mathbf{x}_1) - \phi(\mathbf{x}_2), \mathbf{x}_1 - \mathbf{x}_2 \rangle \end{aligned}$$

where μ and φ are real numbers. Similar results related to the dynamics of multi-machine power systems established a similar quadratic bound on the nonlinear component (see [39]). To determine the constants ρ , μ , and φ , a simple offline algorithm

can be implemented¹. Following this assumption, the dynamics of this observer can be written as

$$\dot{\hat{x}} = A\hat{x} + Bu + \phi(\hat{x}) + L(y - C\hat{x}) \quad (7)$$

where L is a matrix gain determined by Algorithm 3.

Algorithm 3 Observer Design Algorithm

compute constants ρ, μ , and φ via an offline search algorithm
solve this LMI for $\epsilon_1, \epsilon_2, \sigma > 0$ and $P = P^\top \succ O$:

$$\begin{bmatrix} A^\top P + PA + (\epsilon_1 \rho + \epsilon_2 \mu) I_n & -\sigma C^\top C & P + \frac{\varphi \epsilon_2 - \epsilon_1}{2} I_n \\ -\sigma C^\top C & P + \frac{\varphi \epsilon_2 - \epsilon_1}{2} I_n & -\epsilon_2 I_n \end{bmatrix} < 0. \quad (8)$$

obtain the observer design gain matrix L :

$$L = \frac{\sigma}{2} P^{-1} C^\top. \quad (9)$$

simulate observer design given in (7)

First, given the Lipschitz constants ρ, φ , and μ , the linear matrix inequality in (8) is solved for positive constants ϵ_1, ϵ_2 , and σ and a symmetric positive semi-definite matrix P . Utilizing the L in (9), the state estimates generated from (7) are guaranteed to converge to the actual values of the states.

Note that the observer design utilizes linearized measurement functions C , which for power system DSE can be obtained by linearizing the nonlinear functions in (5). However, since the measurement functions have high nonlinearity, when performing the estimation we do not use (7), as in [38], but choose to directly use the nonlinear measurement functions as

$$\dot{\hat{x}} = A\hat{x} + Bu + \phi(\hat{x}) + L(y - h(\hat{x})). \quad (10)$$

VI. NUMERICAL RESULTS

Here we test EKF, SR-UKF, CKF, and the nonlinear observer on the 16-machine 68-bus system extracted from Power System Toolbox (PST) [40]. For the DSE we consider both unknown inputs to the system dynamics and cyber attacks against the measurements including data integrity, DoS, and replay attacks; see Section III. All tests are performed on a 3.2-GHz Intel(R) Core(TM) i7-4790S desktop.

The simulation data is generated as follows.

- 1) The simulation data is generated by the model in Section II with an additional IEEE Type DC1 excitation system and a simplified turbine-governor system for each generator. The sampling rate is 60 samples/s.
- 2) In order to generate dynamic response, a three-phase fault is applied at bus 6 of branch 6 – 11 and is cleared at the near and remote ends after 0.05s and 0.1s.
- 3) All generators are equipped with PMUs.
- 4) The sampling rate of the measurements is set to be 60 frames/s to mimic the PMU sampling rate.

¹These constants can be determined by evaluating the bounds on the nonlinear function $\phi(x, u)$ and adding a possible bound on the unknown inputs and disturbances. Determining those constants affects the design of the observer, and hence it is advised to choose conservative bound-constants on the nonlinear function. The nonlinearities present in the multi-machine power system are bounded (e.g., sines and cosines of angles, multiplications of bounded quantities such as voltages and currents).

- 5) Gaussian process noise is added and the corresponding process noise covariance is set as a diagonal matrix, whose diagonal entries are the square of 5% of the largest state changes [29].
- 6) Gaussian noise with variance 0.01^2 is added to the PMU measurements.
- 7) Each entry of the unknown input coefficients B_w is a random number that follows normal distribution with zero mean and variance as the square of 50% of the largest state changes. Note that the variance here is much bigger than that of the process noise.
- 8) The unknown input vector w is set as a function of t as

$$w(t) = \begin{bmatrix} 0.5 \cos(\omega_u t) \\ 0.5 \sin(\omega_u t) \\ 0.5 \cos(\omega_u t) \\ 0.5 \sin(\omega_u t) \\ -e^{-5t} \\ 0.2 e^{-t} \cos(\omega_u t) \\ 0.2 \cos(\omega_u t) \\ 0.1 \sin(\omega_u t) \end{bmatrix}$$

where $\omega_u = 100$ is the frequency of the given signals. The unknown inputs are manually chosen, showing different scenarios for inaccurate model and parameters without a clear, predetermined known distribution or waveform.

The Kalman filters and the observer are set as follows.

- 1) DSE is performed on the post-contingency system on time period $[0, 10s]$, which starts from the fault clearing.
- 2) The initial estimated mean of the rotor speed is set to be ω_0 and that for the other states is set to be twice of the real initial states.
- 3) The initial estimation error covariance is set to be $0.1 I_n$.
- 4) As mentioned before, the covariance of the process noise is set as a diagonal matrix, whose diagonal entries are the square of 5% of the largest state changes [29].
- 5) The covariance for the measurement noise is a diagonal matrix, whose diagonal entries are 0.01^2 , as in [29].
- 6) For the observer discussed in Section V, the LMI (8) is solved via CVX on MATLAB [41]. The Lipschitz constants in Algorithm 3 are all set to be 1.
- 7) The Kalman filters and the observer only has the power system model in Section II for which T_{mi} and E_{fdi} take steady-state values and on $[0, 1s]$ the reduced admittance matrix \bar{Y} is that for pre-contingency state.
- 8) Data integrity, DoS, and replay attacks, as discussed in Section III-B, are added to the PMU measurements. More details are given in the ensuing sections.

Since the results for different runs of estimation using different methods are very similar, in the following sections we only give results for one estimation.

A. Scenario 1: Data Integrity Attack

Data integrity attack is added to the first eight measurements, i.e., e_{Ri} for $i = 1, \dots, 8$. The compromised measurements are obtained by scaling the real measurements by 0.6 and $1/0.6$, respectively, for the first four and the last four measurements. The 2-norm of the relative error of the states,

$\|(\mathbf{x}(t) - \hat{\mathbf{x}}(t))/\mathbf{x}(t)\|_2$, for different estimation methods is shown in Fig. 1. It is seen that the error norm for both CKF and the observer can quickly converge among which the observer converges faster, while the value that CKF converges to is slightly smaller in magnitude. By contrast, EKF and SR-UKF do not perform well and their error norm cannot converge to small values, which means that the estimates are erroneous.

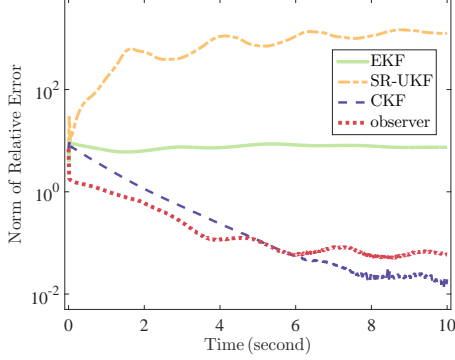


Fig. 1. Norm of relative error of the states in Scenario 1.

We also show the states estimation for Generator 1 in Fig. 2. It is seen that the observer and CKF converge rapidly while the EKF fails to converge after 10 seconds. The estimation for SR-UKF is separately shown in Fig. 3 because its estimated states are far away from the real states. Note that the real system dynamics are stable while the SR-UKF estimation misled by the data integrity attack indicates that the system is unstable.

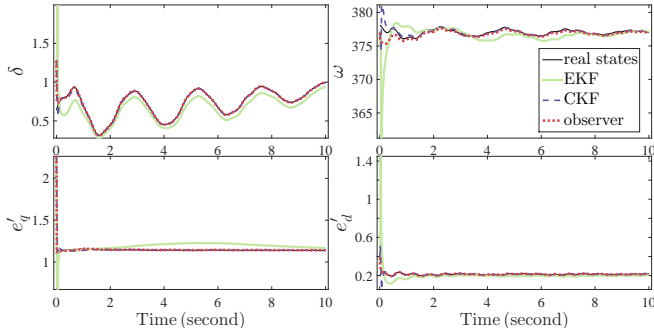


Fig. 2. Estimated states for EKF, CKF, and the observer in Scenario 1.

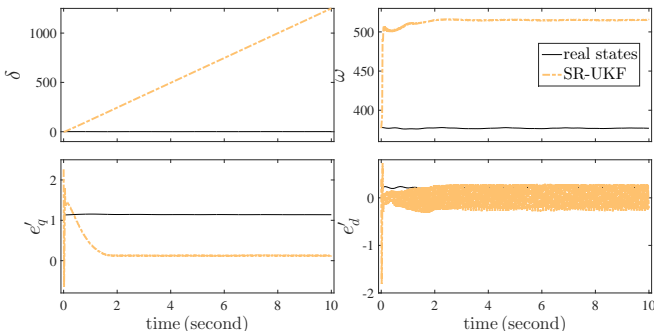


Fig. 3. Estimated states for SR-UKF in Scenario 1.

The real, compromised, and estimated measurements for the

first measurement, e_{R1} , are shown in Fig. 4. For the observer and CKF, the estimated measurements are very close to the actual ones. The results for EKF there show that there are some differences between the estimates and the real values, while SR-UKF's generated estimates are close to the compromised measurements, indicating that SR-UKF is completely misled by the cyber attacks.

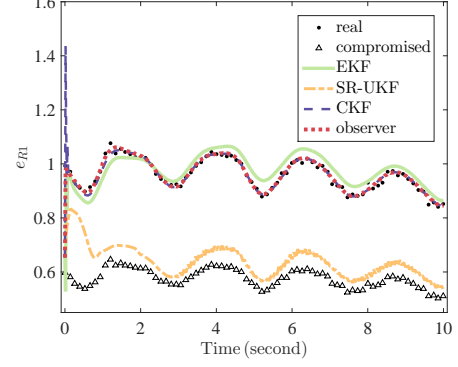


Fig. 4. Estimated measurements for e_{R1} in Scenario 1.

B. Scenario 2: DoS Attack

The first eight measurements are kept unchanged for $t \in [3s, 6s]$ to mimic the DoS attack in which case the updated measurements cannot be sent to the control center due to, for example, jammed communication between PMU to PDC or between PDC to the control center; see NESCOR failure scenarios [34]. The 2-norm of the relative error of the states is shown in Fig. 5 and the results are very similar to those in Scenario 1.

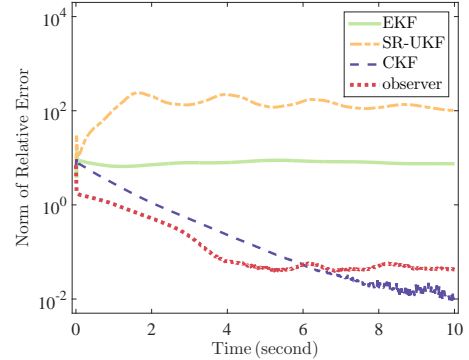


Fig. 5. Norm of relative error of the states in Scenario 2.

Unlike Scenario 1, the estimation for the attacked measurements is not greatly misled by the compromised measurements. However, the estimates generated from EKF and SR-UKF of some measurements that are not attacked are poor. In Fig. 6, for each method, we show the absolute error of the estimated and real measurements for the measurement with the largest 2-norm of the estimation error $\|\hat{y}(t) - y(t)\|_2$ for $t \in [5s, 10s]$, which are the 46th, 43rd, 47th, and 18th measurements, respectively for EKF, SR-UKF, CKF, and the observer. The observer and CKF clearly outperform the other two methods.

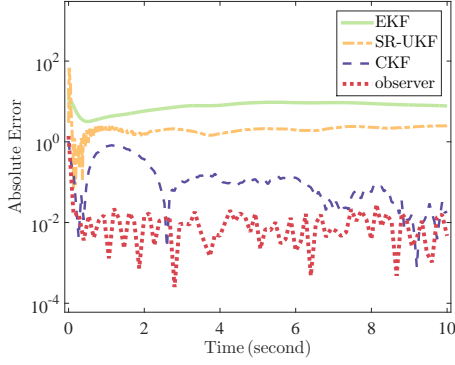


Fig. 6. The absolute error of the measurements in Scenario 2.

C. Scenario 3: Replay Attack

Replay attack is added on the first eight measurements for which there is $y_i(t) = y_i(t - 3)$ for $t \in [3s, 6s]$. The norm of the relative error of the states is shown in Fig. 7, indicating that both CKF and the observer work well while the EKF has the worst performance. Similar to Scenario 2, in Fig. 8 we show the absolute error for the measurement with the largest 2-norm of the estimation error for $t \in [5s, 10s]$, which are the 46th, 43rd, 47th, and 23rd measurements, respectively for EKF, SR-UKF, CKF, and the observer.

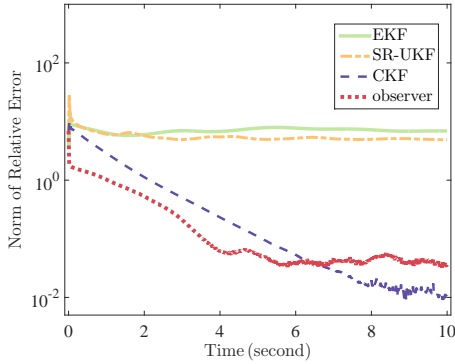


Fig. 7. Norm of relative error of the states in Scenario 3.

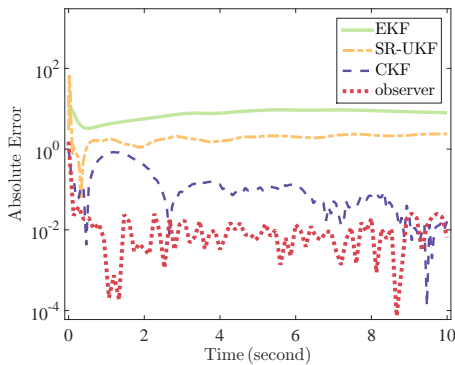


Fig. 8. The absolute error of the measurements in Scenario 3.

D. Computational Efficiency

For the above three scenarios, the average time for estimation by different methods is listed in Table I. It is seen that EKF and the observer are more efficient than the other methods while CKF is the least efficient. Note that the time reported here is from MATLAB implementations. It can be greatly reduced by more efficient, such as C-based implementations.

TABLE I
TIME FOR PERFORMING ESTIMATION FOR 10 SECONDS.

| EKF | SR-UKF | CKF | observer |
|------|--------|-------|----------|
| 6.5s | 15.4s | 64.4s | 10.9s |

VII. COMPARING KALMAN FILTERS AND OBSERVERS

Here, various functionalities of DSE methods and their strengths and weaknesses relative to each functionality are presented based on (a) the technical, theoretical capabilities and (b) experimental results in Section VI.

- *Nonlinearities in the Dynamics:* UKF (SR-UKF), CKF, and the observer in Section V all work on nonlinear systems while EKF assumes linearized system dynamics. Besides, the presented observer uses linearized measurement functions for design but directly uses nonlinear measurement functions for estimation.
- *Solution Feasibility:* The main principle governing the design of most observers is based on finding a matrix gain satisfying a certain condition, such as a solution to a matrix inequality. The state estimates are guaranteed to converge to the actual ones if a solution to the LMI exists. In contrast, KF methods do not require that.
- *Unknown Initial Conditions:* Most observer designs are independent on the knowledge of the initial conditions of the system. However, if the estimator's initial condition is chosen to be reasonably different from the actual one, estimates from KF might not converge to the actual ones.
- *Robustness to Model Uncertainty and Cyber Attacks:* The observer in Section V and the CKF outperforms UKF (SR-UKF) and EKF in the state estimation under model uncertainty and attack vectors.
- *Tolerance to Process and Measurement Noise:* The observer in Section V is tolerant to measurement and process noise similar to the ones assumed for KFs. By design, KF techniques are developed to deal with such noise.
- *Convergence Guarantees:* Observers have theoretical guarantees for convergence while for KF there is no strict proof to guarantee that the estimation converges to actual states.
- *Numerical Stability:* Observers do not have numerical stability problems while the classic UKF can encounter numerical instability because the estimation error covariance matrix is not always guaranteed to be positive semi-definite.
- *Tolerance to Parametric Uncertainty:* KF-based methods can tolerate inaccurate parameters to some extent.

Dynamic observers deal with parametric uncertainty in the sense that all uncertainties can be augmented to the unknown input component in the state dynamics ($B_w w$).

- **Computational Complexity:** The CKF, UKF (SR-UKF), and EKF all have computational complexity of $\mathcal{O}(n^3)$ [16], [26]. Since the observers' matrix gains are obtained offline by solving LMIs, observers are easier to implement as only the dynamics are needed in the estimation.

VIII. CONCLUSION

In this paper, we discuss different DSE methods by presenting an overview of state-of-the-art estimation techniques and developing alternatives, including the cubature Kalman filter and dynamic observers, to address major limitations of existing methods such as intolerance to inaccurate system model and malicious cyber attacks. The proposed methods are tested on a 16-machine 68-bus system, under significant model uncertainty and cyber attacks against the synchrophasor measurements. It is shown that the CKF and the presented observer are more robust to model uncertainty and cyber attacks. Based on both the theoretical, technical capabilities and the experimental results, we summarize the strengths and weaknesses of different estimation techniques especially for power system DSE.

REFERENCES

- [1] F. Schweppe and J. Wildes, "Power system static-state estimation, part I: Exact model," *IEEE Trans. Power App. Syst.*, vol. PAS-89, no. 1, pp. 120–125, Jan. 1970.
- [2] A. Abur and A. Expósito, *Power System State Estimation: Theory and Implementation*, ser. Power Engineering (Willis). CRC Press, 2004.
- [3] A. Monticelli, "Electric power system state estimation," *Proc. IEEE*, vol. 88, no. 2, pp. 262–282, Feb. 2000.
- [4] G. He, S. Dong, J. Qi, and Y. Wang, "Robust state estimator based on maximum normal measurement rate," *IEEE Trans. Power Syst.*, vol. 26, no. 4, pp. 2058–2065, Nov. 2011.
- [5] J. Qi, G. He, S. Mei, and F. Liu, "Power system set membership state estimation," in *IEEE Power and Energy Society General Meeting*, 2012, pp. 1–7.
- [6] K. Zhou, J. C. Doyle, and K. Glover, *Robust and Optimal Control*. Prentice hall New Jersey, 1996.
- [7] Z. Huang, P. Du, D. Kosterev, and S. Yang, "Generator dynamic model validation and parameter calibration using phasor measurements at the point of connection," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1939–1949, 2013.
- [8] A. Hajnoroozi, F. Aminifar, H. Ayoubzadeh *et al.*, "Generating unit model validation and calibration through synchrophasor measurements," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 441–449, 2015.
- [9] M. Ariff, B. Pal, and A. Singh, "Estimating dynamic model parameters for adaptive protection and control in power system," *IEEE Trans. Power Syst.*, vol. 30, no. 2, pp. 829–839, 2015.
- [10] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 21–32.
- [11] S. Mousavian, J. Valenzuela, and J. Wang, "A probabilistic risk mitigation model for cyber-attacks to PMU networks," *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 156–165, Jan. 2015.
- [12] R. E. Kalman, "A new approach to linear filtering and prediction problems," *J. Fluids Eng.*, vol. 82, no. 1, pp. 35–45, 1960.
- [13] A. H. Jazwinski, *Stochastic Processes and Filtering Theory*. Courier Corporation, 2007.
- [14] S. J. Julier and J. K. Uhlmann, "New extension of the Kalman filter to nonlinear systems," pp. 182–193, 1997.
- [15] S. Julier and J. Uhlmann, "Unscented filtering and nonlinear estimation," *Proc. IEEE*, vol. 92, no. 3, pp. 401–422, Mar. 2004.
- [16] I. Arasaratnam and S. Haykin, "Cubature Kalman filters," *IEEE Trans. Autom. Control*, vol. 54, no. 6, pp. 1254–1269, Jun. 2009.
- [17] W. Kang, A. J. Krener, M. Xiao, and L. Xu, *Data Assimilation for Atmospheric, Oceanic and Hydrologic Applications (Vol. II)*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, ch. A Survey of Observers for Nonlinear Dynamical Systems, pp. 1–25.
- [18] A. Radke and Z. Gao, "A survey of state and disturbance observers for practitioners," in *American Control Conference*, Jun. 2006.
- [19] Z. Hidayat, R. Babuska, B. D. Schutter, and A. Nez, "Observers for linear distributed-parameter systems: A survey," in *IEEE International Symposium on Robot and Sensors Environments (ROSE)*, Sept. 2011, pp. 166–171.
- [20] Z. Huang, K. Schneider, and J. Nieplocha, "Feasibility studies of applying Kalman filter techniques to power system dynamic state estimation," in *Proc. 2007 Power Engineering Conf.*, Dec. 2007, pp. 376–382.
- [21] E. Ghahremani and I. Kamwa, "Dynamic state estimation in power system by applying the extended Kalman filter with unknown inputs to phasor measurements," *IEEE Trans. Power Syst.*, vol. 26, no. 4, pp. 2556–2566, Nov. 2011.
- [22] S. Wang, W. Gao, and A. Meliopoulos, "An alternative method for power system dynamic state estimation based on unscented transform," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 942–950, May 2012.
- [23] E. Ghahremani and I. Kamwa, "Online state estimation of a synchronous generator using unscented Kalman filter from phasor measurements units," *IEEE Trans. Energy Convers.*, vol. 26, no. 4, pp. 1099–1108, 2011.
- [24] A. Singh and B. Pal, "Decentralized dynamic state estimation in power systems using unscented transformation," *IEEE Trans. Power Syst.*, vol. 29, no. 2, pp. 794–804, Mar. 2014.
- [25] K. Sun, J. Qi, and W. Kang, "Power system observability and dynamic state estimation for stability monitoring using synchrophasor measurements," *Control Engineering Practice*, 2016.
- [26] R. Van Der Merwe and E. A. Wan, "The square-root unscented Kalman filter for state and parameter-estimation," in *Proc. Int. Conf. Acoustics, Speech, and Signal Processing*, vol. 6, 2001, pp. 3461–3464.
- [27] J. Qi, K. Sun, and W. Kang, "Optimal PMU placement for power system dynamic state estimation by using empirical observability gramian," *IEEE Trans. Power Syst.*, vol. 30, no. 4, pp. 2041–2054, Jul. 2015.
- [28] J. Qi, K. Sun, J. Wang, and H. Liu, "Dynamic state estimation for multi-machine power system by unscented Kalman filter with enhanced numerical stability," *arXiv preprint arXiv:1509.07394*, 2015.
- [29] N. Zhou, D. Meng, and S. Lu, "Estimation of the dynamic states of synchronous machines using an extended particle filter," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4152–4161, Nov. 2013.
- [30] Y. Cui and R. Kavasseri, "A particle filter for dynamic state estimation in multi-machine systems with detailed models," *IEEE Trans. Power Syst.*, vol. 30, no. 6, pp. 3377–3385, Nov. 2015.
- [31] N. Zhou, D. Meng, Z. Huang, and G. Welch, "Dynamic state estimation of a synchronous machine using pmu data: A comparative study," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 450–460, Jan. 2015.
- [32] J. Chen and R. Patton, *Robust Model-Based Fault Diagnosis for Dynamic Systems*. Springer Publishing Company, Incorporated, 2012.
- [33] A. Pertew, H. Marquez, and Q. Zhao, "Design of unknown input observers for lipschitz nonlinear systems," in *Proc. American Control Conf.*, Jun. 2005, pp. 4198–4203.
- [34] "Electric Sector Failure Scenarios and Impact Analyses," Electric Power Research Institute (EPRI), Tech. Rep., Jun. 2014.
- [35] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, 2012.
- [36] J. K. Uhlmann, "Simultaneous map building and localization for real time applications," *transfer thesis, Univ. Oxford, Oxford, UK*, 1994.
- [37] R. Bellman and R. Bellman, *Adaptive Control Processes: A Guided Tour*, ser. Rand Corporation. Research studies. Princeton University Press, 1961.
- [38] W. Zhang, H. Su, H. Wang, and Z. Han, "Full-order and reduced-order observers for one-sided lipschitz nonlinear systems using riccati equations," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 12, pp. 4968–4977, 2012.
- [39] D. Siljak, D. Stipanovic, and A. Zecevic, "Robust decentralized turbine/governor control using linear matrix inequalities," *IEEE Trans. Power Syst.*, vol. 17, no. 3, pp. 715–722, Aug. 2002.
- [40] J. H. Chow and K. W. Cheung, "A toolbox for power system dynamics and control engineering education and research," *IEEE Trans. Power Syst.*, vol. 7, no. 4, pp. 1559–1564, 1992.
- [41] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming," Tech. Rep., Sept. 2013.